What Is Claimed Is:

1. A method to facilitate secure messaging, comprising:

creating a message at an origin;

computing a digest of the message;

signing the digest using an origin private encryption key;

sending the message and the digest to a queue for delivery to a recipient;

receiving the message and the digest at the queue;

verifying that the digest was signed at the origin by using an origin public encryption key, whereby the origin cannot deny creating the message; and

if the digest is verified as being signed at the origin,

placing the message and digest on the queue, and

notifying the recipient that the message is available.

2. The method of claim 1, further comprising:

generating a request at the recipient to receive the message from the queue;

creating a signature for the request using a recipient private encryption key;

sending the request and the signature to the queue;

validating the request at the queue using the signature and a recipient public encryption key; and

if the request is valid,

dequeueing the message from the queue,

sending the digest to the recipient;

signing the digest at the recipient using the recipient private encryption key creating a signed digest;

returning the signed digest to the queue, validating the signed digest at the queue using the recipient public encryption key, whereby the recipient cannot deny requesting to receive the message, and

if the signed digest is valid, sending the message to the recipient.

3. The method of claim 2, further comprising passing the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

4. The method of claim 3, further comprising passing the message and the digest through a plurality of databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

5. The method of claim 2, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

6. The method of claim 2, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

7. The method of claim 2, wherein computing the digest includes using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

8. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to facilitate secure messaging, the method comprising:

creating a message at an origin;

computing a digest of the message;

signing the digest using an origin private encryption key;

sending the message and the digest to a queue for delivery to a recipient;

receiving the message and the digest at the queue;

verifying that the digest was signed at the origin by using an origin public encryption key, whereby the origin cannot deny creating the message; and

if the digest is verified as being signed at the origin,

placing the message and digest on the queue, and

notifying the recipient that the message is available.

9. The computer-readable storage medium of claim 8, the method further comprising:

generating a request at the recipient to receive the message from the queue;

creating a signature for the request using a recipient private encryption key;

sending the request and the signature to the queue;

validating the request at the queue using the signature and a recipient public encryption key; and

if the request is valid,

dequeueing the message from the queue,

sending the digest to the recipient,

signing the digest at the recipient using the recipient private encryption key creating a signed digest, returning the signed digest to the queue,

validating the signed digest at the queue using the recipient public encryption key, whereby the recipient cannot deny requesting to receive the message, and

if the signed digest is valid, sending the message to the recipient.

10. The computer-readable storage medium of claim 9, the method further comprising passing the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

11. The computer-readable storage medium of claim 10, the method further comprising passing the message and the digest through a plurality of databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

12. The computer-readable storage medium of claim 9, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

13. The computer-readable storage medium of claim 9, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

14. The computer-readable storage medium of claim 9, wherein computing the digest includes using one of message digest 2 (MD2), message

digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

15. An apparatus to facilitate secure messaging, comprising:

a first creating mechanism that is configured to create a message at an origin;

a computing mechanism that is configured to compute a digest of the message;

a first signing mechanism that is configured to sign the digest using an origin private encryption key;

a first sending mechanism that is configured to send the message and the digest to a queue for delivery to a recipient;

a receiving mechanism that is configured to receive the message and the digest at the queue;

a verifying mechanism that is configured to verify that the digest was signed at the origin by using an origin public encryption key, whereby the origin cannot deny creating the message;

a placing mechanism that is configured to place the message and digest on the queue; and

a notifying mechanism that is configured to notify the recipient that the message is available.

16. The apparatus of claim 15, further comprising:

a generating mechanism that is configured to generate a request at the recipient to receive the message from the queue;

a second creating mechanism that is configured to create a signature for the request using a recipient private encryption key;

a second sending mechanism that is configured to send the request and the signature to the queue;

a first validating mechanism that is configured to validate the request at the queue using the signature and a recipient public encryption key;

a dequeueing mechanism that is configured to dequeue the message from the queue;

a third sending mechanism that is configured to send the digest to the recipient;

a second signing mechanism that is configured to sign the digest at the recipient using the recipient private encryption key creating a signed digest;

a returning mechanism that is configured to return the signed digest to the queue;

a second validating mechanism that is configured to validate the signed digest at the queue using the recipient public encryption key, whereby the recipient cannot deny requesting to receive the message; and

wherein the third sending mechanism is further configured to send the message to the recipient.

17. The apparatus of claim 16, further comprising a passing mechanism that is configured to pass the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

18. The apparatus of claim 17, wherein the passing mechanism is further configured to pass the message and the digest through a plurality of databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

19. The apparatus of claim 16, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

20. The apparatus of claim 16, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

21. The apparatus of claim 16, wherein computing the digest includes using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).